KOLARI
KASVAA
LUONNOSTA

Kolarin kunnan tietosuojapolitiikka

Kunnanhallitus 8.5.2018

KOLARI
KASVAA
LUONNOSTA

Sisällys

1. Johdanto

Tietosuojapolitiikka on tietosuojatyöryhmän laatima ja kunnanhallituksen hyväksymä asiakirja, joka on ohjeistus tietosuojan kehittämiseen ja ylläpitämiseen. Tämä asiakirja on itse tietosuoja-asetuksen (GDPR) lisäksi ylin tietosuojaa ohjaava dokumentti. Tietosuojapolitiikan tavoitteena on luoda Kolarin kunnan kaikille toimialoille yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän ja turvallisen henkilötietojen käsittelyn, säilönnän ja prosessoinnin takaamiseksi (tietoturvatason toteuttamiseksi). Kehitysehdotuksia ja riskejä eri toimialoilta voi esittää tietosuojatyöryhmälle.

Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste. Kolarin kunnassa henkilötietojen käsittely on tarpeen rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseksi, yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

Kolarin kunta noudattaa tietosuojassa riskiperusteista lähestymistapaa. Tämä tarkoittaa, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Riski voi olla korkeampi silloin, kun käsitellään esimerkiksi erityisiä (arkaluontoisia) henkilötietoja, heikommassa asemassa olevien tietoja tai suuria määriä henkilötietoja. Kolarin kunta rekisterinpitäjänä arvioi perusteellisesti henkilötietojen käsittelyyn liittyvät riskit, jotta tietosuoja-asetuksen sisäänrakennettu ja oletusarvoinen tietosuoja sekä muut säädetyt velvollisuudet toteutuisivat.

2. Käsitteet

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvä tieto. Tunnistettavissa olevalla tarkoitetaan luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tietojen perusteella. Henkilötietoa on näin ollen muun muassa henkilön nimi, henkilötunnus, sijaintitieto ja yhden tai useamman hänelle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä, joiden perusteella henkilön voi tunnistaa.

Henkilötietojen käsittely

Kaikenlainen toiminta tai toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Henkilötietojen käsittelynä pidetään muun muassa tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne

muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Henkilötietojen käsittelijä

Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötietorekisteri

Mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot on saatavilla tietyin perustein.

Rekisterinpitäjä

Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity

Henkilö, jonka tietoja käsitellään.

3. Tietosuoja

3.1 Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on oltava asianmukaista ja sille on aina oltava käsittelyperuste. Henkilötietojen suojalla tarkoitetaan jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot korjatuiksi, mikäli tietojen oikaisu on tarpeen.

3.2 Tietosuojan tavoitteet ja periaatteet

EU:n yleinen tietosuoja-asetus muodostaa perustan Kolarin kunnan henkilötietojen käsittelylle. Asetuksen periaatteet ohjaavat henkilötietojen käyttöä ja turvaavat rekisteröityjen oikeuksia. Henkilötietojen käsittelyssä noudatetaan seuraavia periaatteita:

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys: henkilötietoja käsitellään lainmukaisesti kohtuullisesti ja rekisteröidyn kannalta läpinäkyvästi. Rekisteröidylle tulee olla läpinäkyvää, miten heitä koskevia tietoja kerätään ja käsitellään ja mihin tietoja kerätään.

Käyttötarkoitussidonnaisuus: henkilötietojen kerätään vain tiettyä käyttötarkoitusta varten eikä niitä käytetä myöhemmin tarkoitukseen, jolla ei ole sidonnaisuutta kerättyyn käyttötarkoitukseen.

Tietojen minimointi: henkilötietojen kerääminen rajataan ja minimoidaan suhteessa keräämisen tarkoitukseen ja henkilötietojen ovat asianmukaisia ja olennaisia.

Täsmällisyys: henkilötiedot ovat täsmällisiä ja mahdolliset virheelliset tiedot korjataan viipymättä.

Säilytyksen rajoittaminen: tietoja säilytetään henkilön tunnistettavassa muodossa niin kauan kuin se on tarpeen tietojen käsittelyn kannalta.

Eheys ja luottamuksellisuus: henkilötietojen käsittelyssä varmistetaan tietojen eheys ja luottamuksellisuus. Tietoja suojataan teknisin ja organisatorisin keinoin luvattomalta ja lainvastaiselta käsittelyltä, häviämiseltä ja tuhoutumiselta.

Rekisterinpitäjän osoitusvelvollisuus: rekisterinpitäjä on sitoutunut noudattamaan asetusta ja sen periaatteita ja dokumentoimaan toimet, joilla tietosuojaa toteutetaan oletusarvoisesti ja sisäänrakennetusti.

3.3 Oletusarvoinen ja sisäänrakennettu tietosuoja

Kolarin kunnan tavoitteena on luoda oletusarvoinen ja sisäänrakennettu tietosuoja. Tällä tarkoitetaan sitä, että organisaation alkaa toimia tietosuoja-asetuksen vaatimusten mukaisesti päivittäisessä toiminnassaan. Kolarin kunta käyttää toiminnassaan nykyaikaista ja tietoturvallista teknologiaa riskiperusteisuus huomioon ottaen. Henkilöstölle tarjotaan koulutusta ja ohjeistuksia tietoturvaan ja tietosuojaan liittyen.

Kolarin kunta käyttää tietosuoja-asetuksen asettamien vaatimusten dokumentointiin erillistä ohjelmaa. Ohjelmaan on listattu Kolarin kunnassa käytössä olevat tietojärjestelmät ja tietovirrat. Tietohallinto ja tietosuojaryhmä ovat käyneet nämä läpi keskitetysti yhdessä järjestelmien pääkäyttäjien kanssa, jotka tuntevat järjestelmien toiminnallisuudet parhaiten. Tietosuojaan liittyvää vastuuta on jaettu myös pääkäyttäjille. Pääkäyttäjät ovat listattuna myös ohjelman tietojärjestelmäsalkkuun. Ohjelmaan on koottu eri järjestelmien sisältämät henkilötiedot sekä rekisteri/tietosuojaselosteet. Ohjelmasta löytyvät ohjeistukset muun muassa sopimuksille, hankintojen kilpailutukselle ja projekteille.

Tietosuoja-asetus huomioidaan julkisten hankintojen kilpailutuksessa. Olemassa olevat sopimukset käydään läpi ja päivitetään vastaamaan tietosuoja-asetuksen vaatimuksia. Uusissa sopimuksissa toimitaan tietosuoja-asetuksen vaatimusten mukaisesti. Tietosuoja-asetus huomioidaan myös kaikissa uusissa projekteissa.

Henkilöstö koulutetaan tuntemaan tietosuoja-asetuksen sisältö. Tämä koskee erityisesti henkilötietoja käsitteleviä työntekijöitä ja viranhaltijoita. Lisäksi ulkopuolisilta henkilötietojen käsittelijöiltä odotetaan asetuksen mukaista tietojenkäsittelyä.

Ohjeistuksien tulee olla kaikkien saatavilla. Henkilötietojen käsittelyä valvotaan asetuksessa edellyttämällä tavalla. Kaikki tietosuojan toteuttamiseen liittyvät toimenpiteet dokumentoidaan.

3.4 Rekisteröidyn oikeudet

Rekisterinpitäjällä on velvollisuus informoida rekisteröityjä tietojen käsittelystä. Tiedot on esitettävä tiiviisti läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Kolarin kunta informoi rekisteröityjä lähtökohtaisesti verkkosivuillaan ja toimipisteillään. Rekisteröidyllä on oikeus saada vahvistus siitä, käsitelläänkö häntä koskevia tietoja ja jos käsitellään, hänellä on oikeus saada tiedot itselleen. Rekisteröidyllä on oikeus tietojensa korjaamiseen ja rajoittamiseen.

Lisäksi rekisteröidyllä on oikeus saada tieto mahdollisesta tietoturvaloukkauksesta, mikäli loukkaus aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille.

Kolarin kunta on luonut prosessit, jotta rekisteröityjen oikeudet toteutuisivat. Prosesseja kehitetään säännöllisesti.

4. Tietosuojaorganisaatio

Kunnanhallitus hyväksyy tietosuojapolitiikan ja vastaa tarvittavien edellytysten luomisesta niiden toteuttamiseksi.

Henkilötietojen käsittelyn lainmukaisuudesta vastaa kunnan johto. Johdon vastuulla on huolehtia tietosuojan ja tietoturvan riittävästä resursoinnista ja siitä, että se on oletusarvoista ja sisäänrakennettua.

Toimialajohtajat huolehtivat omalla toimialallaan tietosuojan lainmukaisuudesta yhdessä esimiesten kanssa. Jokaisen esimiehen on varmistettava, että tietosuoja- ja tietoturvaohjeistukset sekä tietoverkon käyttösäännöt ovat henkilöstön hallussa ja että jokainen käy tietosuojaan liittyvän koulutuspäivän.

Tietosuojatyöryhmä ja tietosuojavastaava toimivat tietosuoja-asioissa asiantuntijoina. Tietosuojaryhmä ja tietosuojavastaava kehittävät organisaation tietosuojaa. Mikäli henkilöstön jäsen huomaa toiminnassa, järjestelmissä tai prosesseissa henkilötietojen käsittelyyn liittyviä ongelmia, vaaroja tms. voi hän ottaa luottamuksellisesti yhteyttä tietosuojavastaavaan tai tietosuojatyöryhmään.

IT vastaa teknisen tietoturvan kehittämisestä, tietojärjestelmien toiminnasta, päivittämisestä ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien osalta.

Kunnan koko henkilöstö on vastuussa siitä, että noudattaa annettuja tietosuoja- ja tietoturvaohjeistuksia. Jokaisella on myös velvollisuus ilmoittaa havaitsemistaan puutteista ja väärinkäytöksistä tietosuojavastaavalle.

4.1 Yhteistyö viranomaisten kanssa

Rekisterinpitäjällä on velvollisuus toimia yhteistyössä valvontaviranomaisen kanssa heidän niin pyytäessä. Henkilötietojen vaihto on tältä osin lainsäädäntöön perustuvaa.

Tietosuojavaltuutettu on viranomainen, joka ohjaa, neuvoo ja valvoo henkilötietojen käsittelyä henkilötietolain mukaisesti. Tietosuojavaltuutettu käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröityjen oikeuksien toteutumisesta.

4.2 Tietoturvaloukkauksiin valmistautuminen

Rekisterinpitäjän velvollisuutena on ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojeluviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Rekisterinpitäjä on sitoutunut ilmoittamaan valvontaviranomaiselle loukkauksesta 72 tunnin kuluessa loukkauksen ilmitulosta. Rekisterinpitäjä on velvollinen ilmoittamaan loukkauksesta myös rekisteröidylle, mikäli loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille. Rekisterinpitäjä dokumentoi kaikki henkilötietojen tietoturvaloukkaukset.